



Setting Up Keeper Security: A Password Management Service

This document serves as a comprehensive guide for setting up Keeper Security, a robust password management service designed to enhance security and streamline password management for ITGuys clients. It includes step-by-step instructions on creating accounts, setting up records, and utilizing various features of Keeper Security. Accompanying graphics will provide visual assistance to ensure a smooth onboarding experience.

[Video: Keeper Overview](#)



Table of Contents

1. Creating your Keeper Security Account
2. Creating Your Master Password
3. Importing Your Passwords
4. Installing the Web Browser Extension
5. Enabling Two-Factor Authentication (2FA)
6. Setting Up Account Recovery
7. Creating and Managing Records
8. Sharing Passwords Securely
9. Keeper's Security Audit Function
10. Final Notes

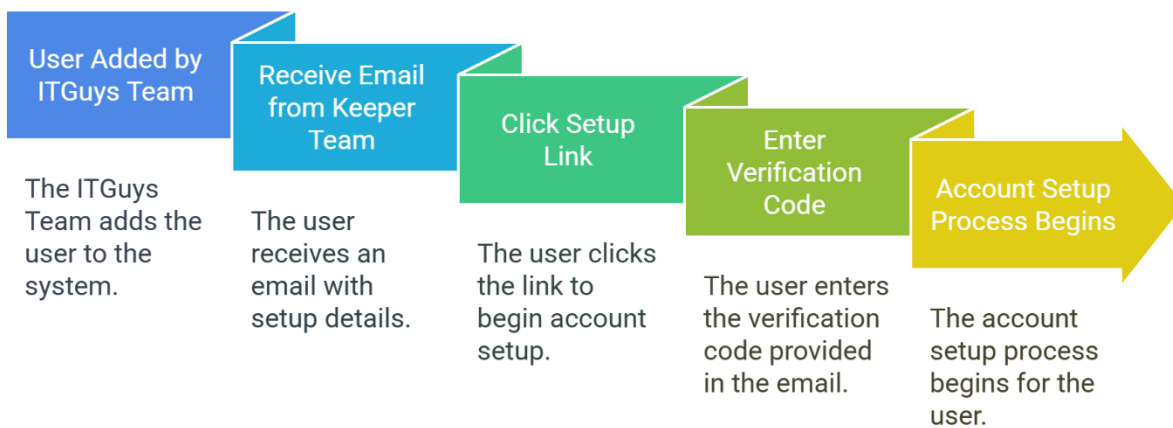


Creating Your Keeper Security Account

1. Setting Up Your Keeper Security Account

When added as a user by the ITGuys Team, you will receive an email from Keeper Team that includes a link and a verification code to set up your new account. Click the **“Set Up Your Account Now”** button.

Video: Keeper Account Creation



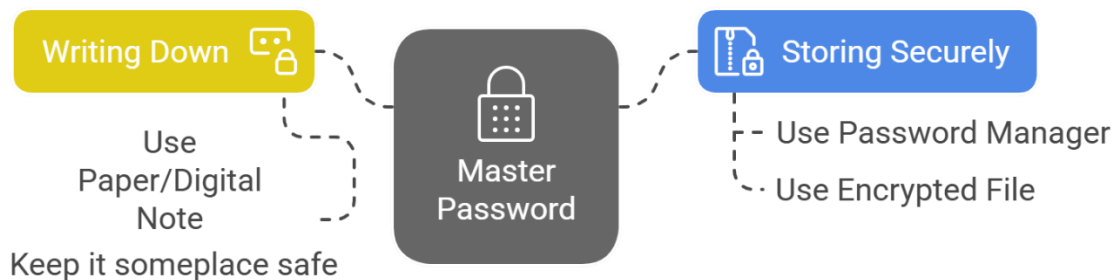
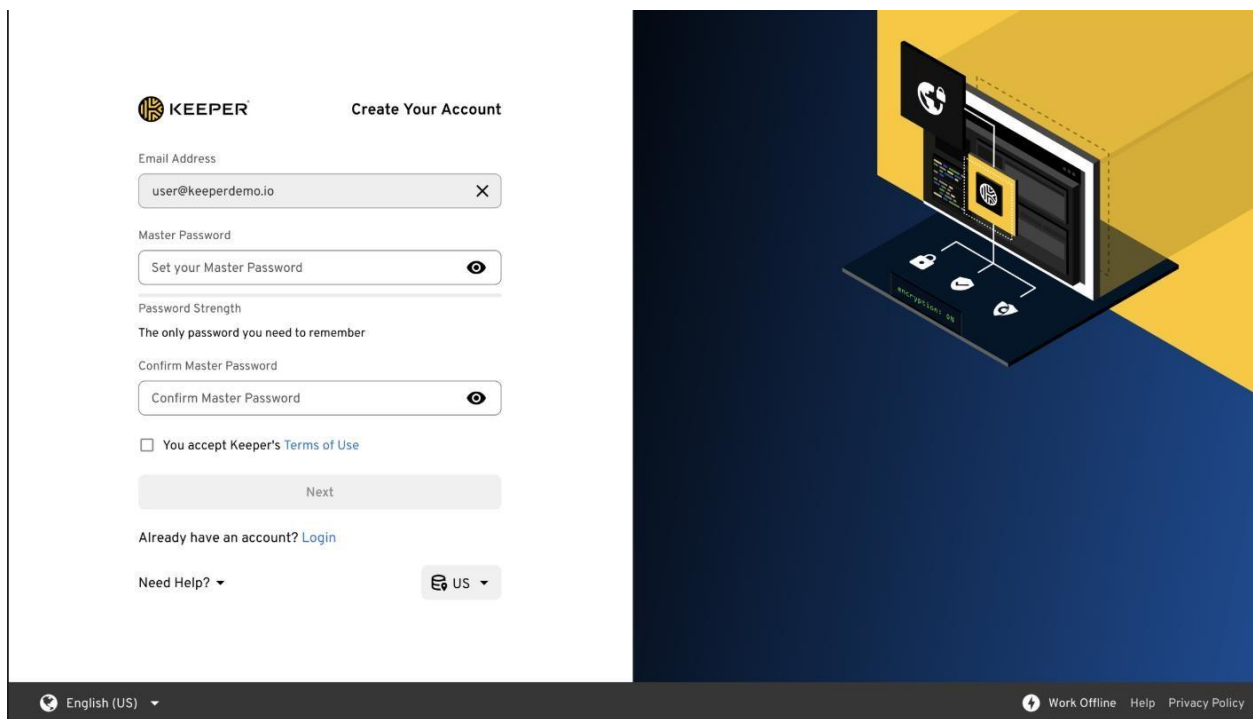
2. Create Your Password

After clicking the “**Set Up Your Account**” button in your email, Keeper will take you to its login page where you will finish inputting your information and create your master password. This will be your personal login to Keeper.

Your master password is the key to your entire vault. Choose a strong, memorable password with 12 characters and a mix of uppercase and lowercase letters, numbers, and special characters.

Confirm Your Master Password: After entering your master password, re-enter it to confirm.

Important: Write down your master password and store it securely



3. Import Your Passwords

After setting your master password, log in to your Keeper vault. On the dashboard, click on the **"Import"** option (also found in the settings menu). Keeper supports various methods to import passwords, such as uploading a CSV file from another password manager, importing from your browser's saved passwords, or syncing from other apps.

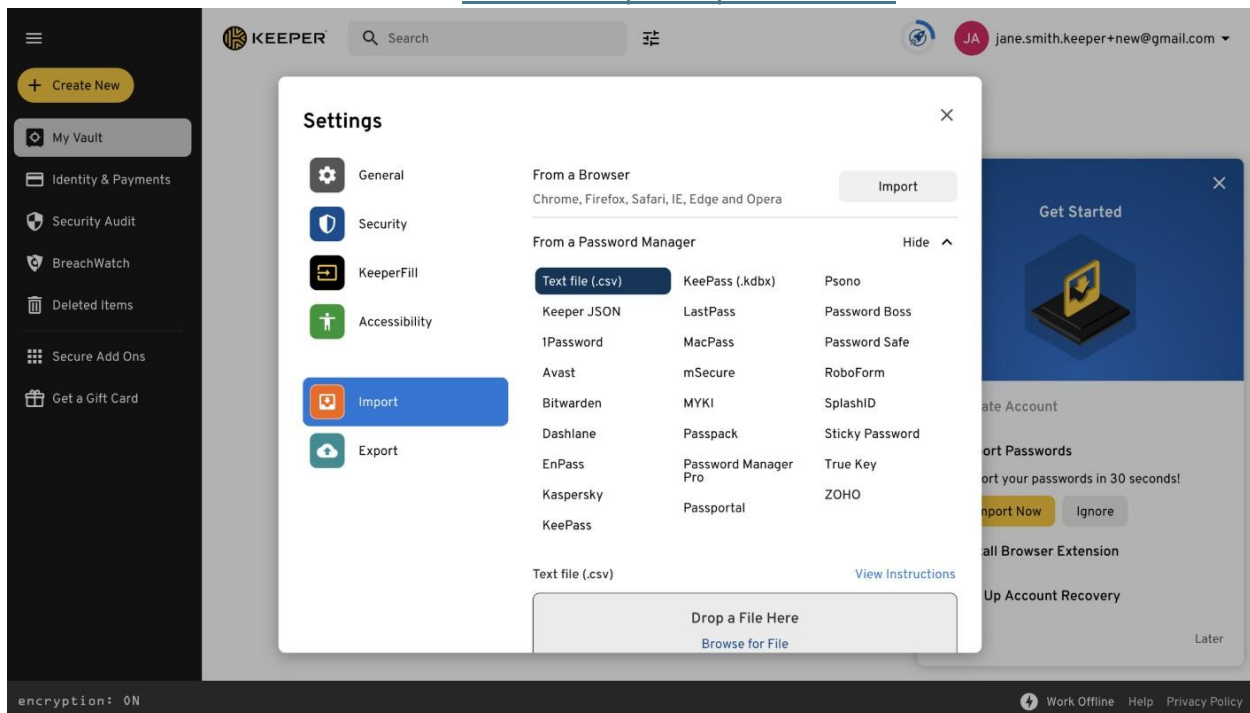
Complete the Import Process:

Follow the on-screen prompts to select your preferred import method and complete the process. It will prompt you to install the **Keeper Import Tool**. The import tool will download to the downloads folder on your computer. While the tool is downloading, **copy the code** that is displayed by clicking on the copy icon. You will be prompted to **paste this code into the field provided** on the Keeper import screen. Then click **"Import."**

Keeper will show you all of the found passwords, then you can select which passwords you'd like to import by checking/unchecking the boxes, then adding them to Keeper with the button on the bottom that says, **"Add to Keeper."**

Note: Imported passwords will be securely stored in your vault.

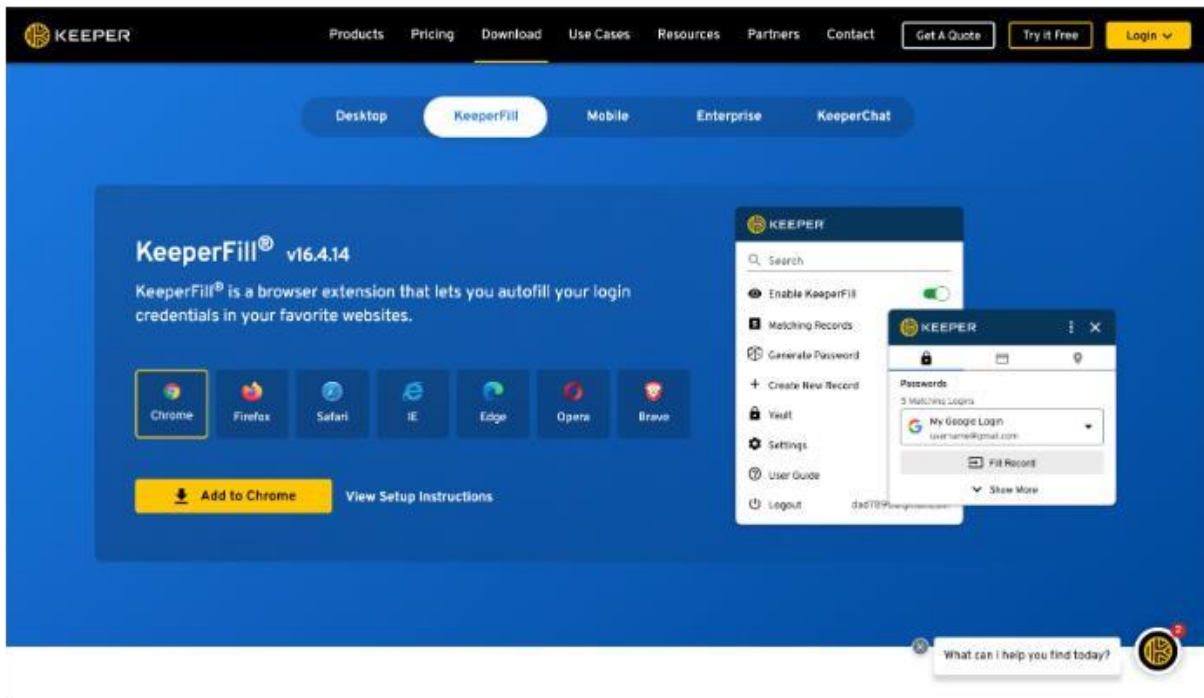
[Video: Keeper Import Process](#)



4. Install the KeeperFill Web Browser Extension

KeeperFill is a secure browser extension that lets you autofill your login credentials on your favorite websites. It can be installed on browsers such as Chrome, Edge, Firefox, Safari, Opera, and other Chromium-based browsers such as Brave.

[Link: KeeperFill Browser Extension Installation Instructions per Browser](#)



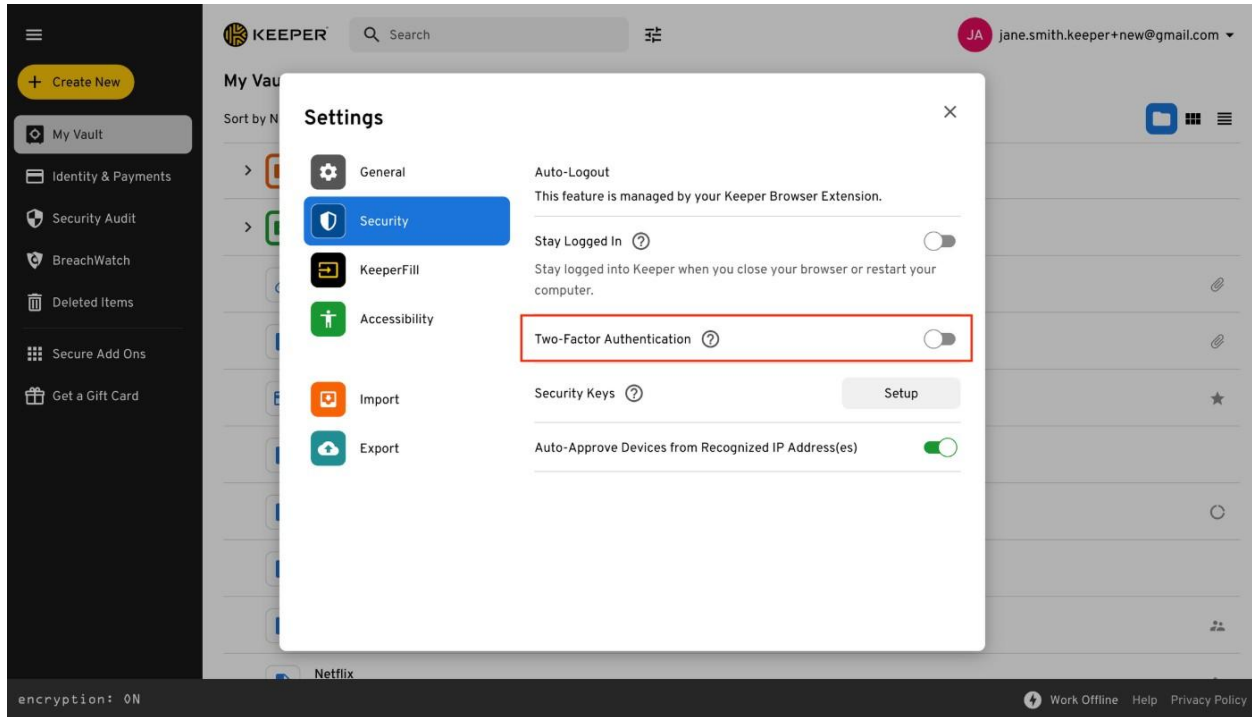
Once installed, open the extension from your browser toolbar and log in with your master password.

After logging in, **enable the autofill feature** in your browser extension so Keeper can automatically fill in your passwords on websites.

5. Enabling Two-Factor Authentication (2FA)

Two-Factor Authentication (2FA) adds an extra layer of security to your vault by requiring a second passcode upon logging in. Some 2FA methods like Duo or RSA require admin configuration. Others, like Google or Microsoft Authenticator Apps, can be set up by individual end-users.

Click the **Account Dropdown Menu** (your email address) then click **Settings > Security** to enable 2FA for your vault.

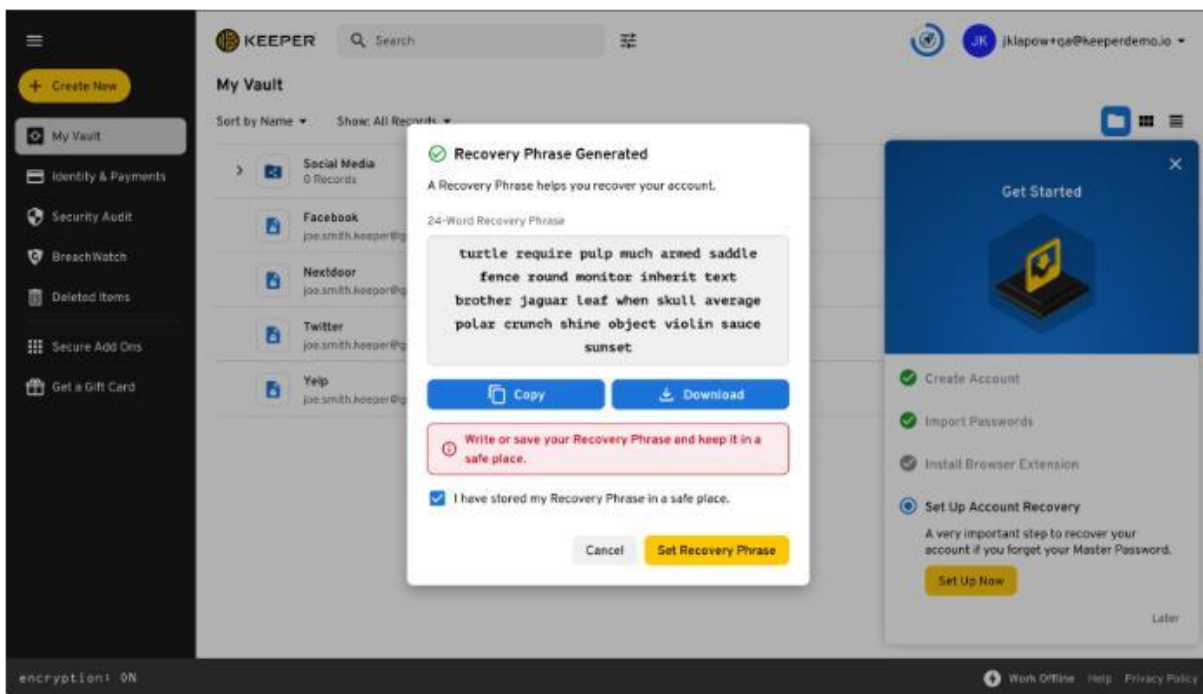
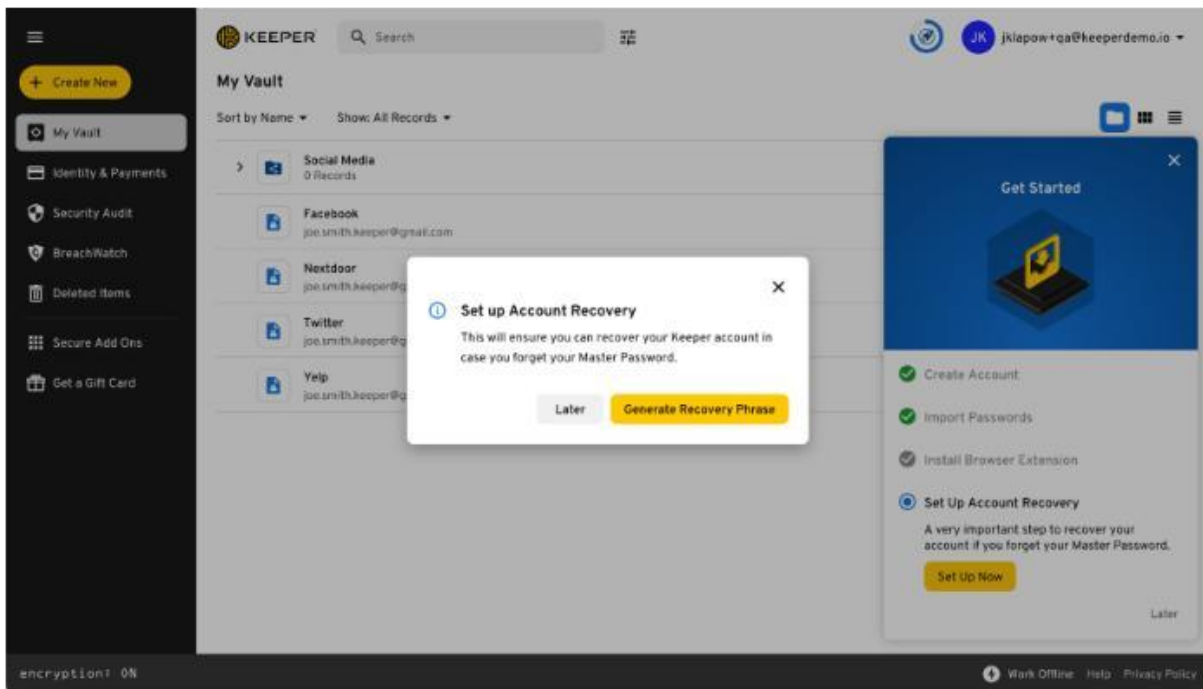


Follow the instructions for your chosen 2FA method. If using an authenticator app, scan the QR code provided by Keeper and enter the verification code.

Important: Once 2FA is enabled, you'll be required to enter the code from your chosen 2FA method each time you log in.

6. Setting Up Account Recovery

Upon initial vault login, new users will be prompted to set up Account Recovery. Click **“Generate Recovery Phrase”** to begin.



Keeper will guide you through setting up a **recovery phrase**. Once your recovery phrase has been generated, **be sure to store it in a safe place**. For added convenience, you will be given the option to copy or download it. Check the box to acknowledge you have stored it in a safe place and click **Set Recovery Phrase** to complete the setup.

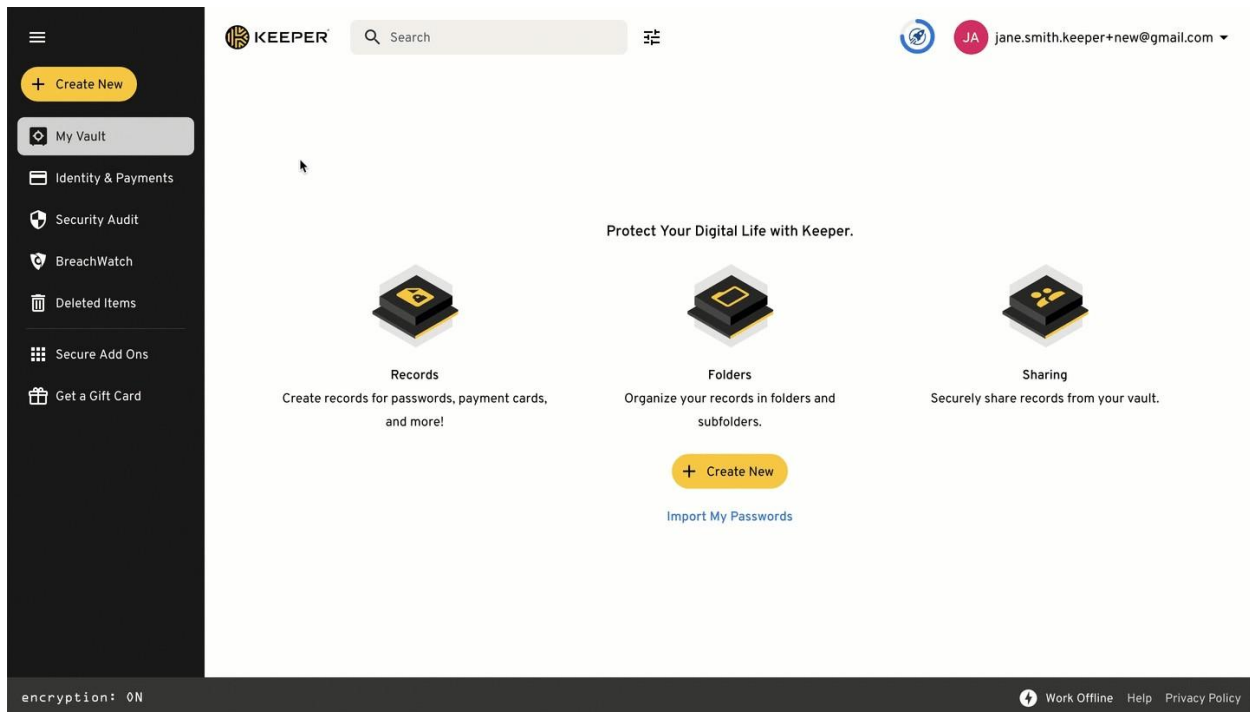


Please note that if you forget your master password and lose your recovery phrase, you will not be able to login to your vault and Keeper Support will be unable to help you regain access.

Creating and Managing Records and Folders

1. Creating A Record

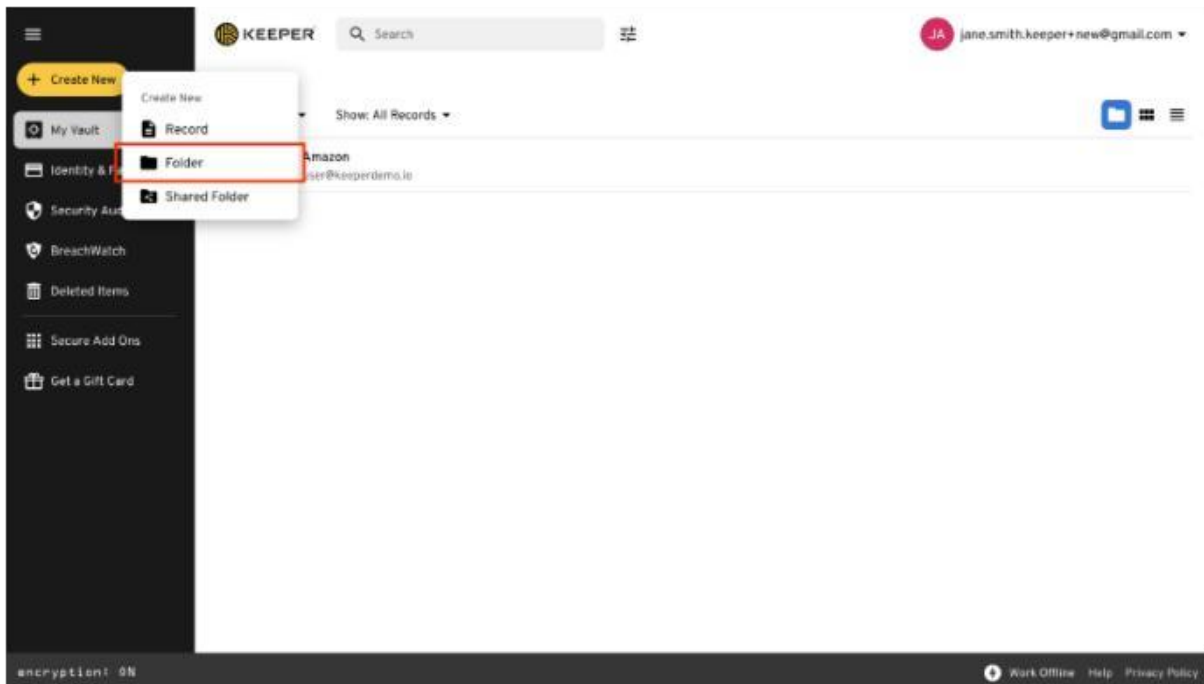
- Click + Create New > **Record**.
- Choose a Record Type from the dropdown menu ("Login" is the default type) (Other types of records include addresses, bank accounts, payment cards, birth certificates, contacts, databases, driver's licenses, secure notes, file attachments, general, health insurances, memberships, passports, photos, servers, software licenses, SSH keys, and identity cards.)
- Enter a name for the Record and click **Next**.
- Enter the Login (Username or Email)
- Enter the Password or click the dice icon to generate one (more on that here)
- Enter the Website Address
- Enter Notes, add Files & Photos, a Two-Factor Code and Custom Fields
- Click **Save** to finish.



2. Creating a Folder

- Click + Create New > **Folder**.
- Enter the name of the folder and click **Create**.
- Drag-and-drop the record(s) you would like to store in the folder and click **Move** or **Create shortcut**.

[Link: Keeper Create a Folder](#)



3. Creating a Subfolder

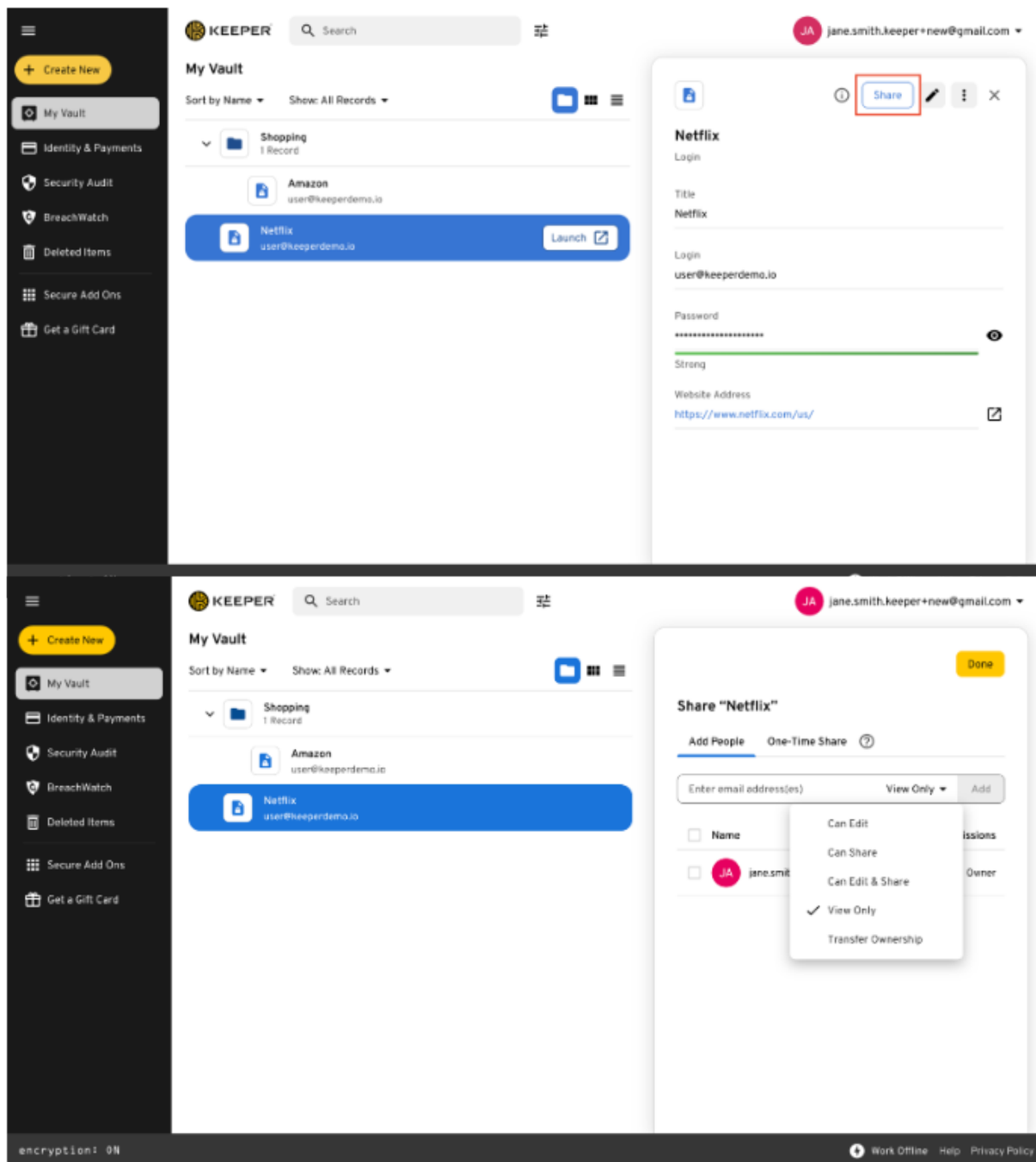
- Right-click on an existing folder and click **New Folder**.
- Enter the name of the subfolder and click **Create**.
- Drag-and-drop the record(s) you would like to store in the subfolder and click **Move** or **Create shortcut**.

Sharing Passwords Securely

Securely create, share, and manage records with family, friends and colleagues.

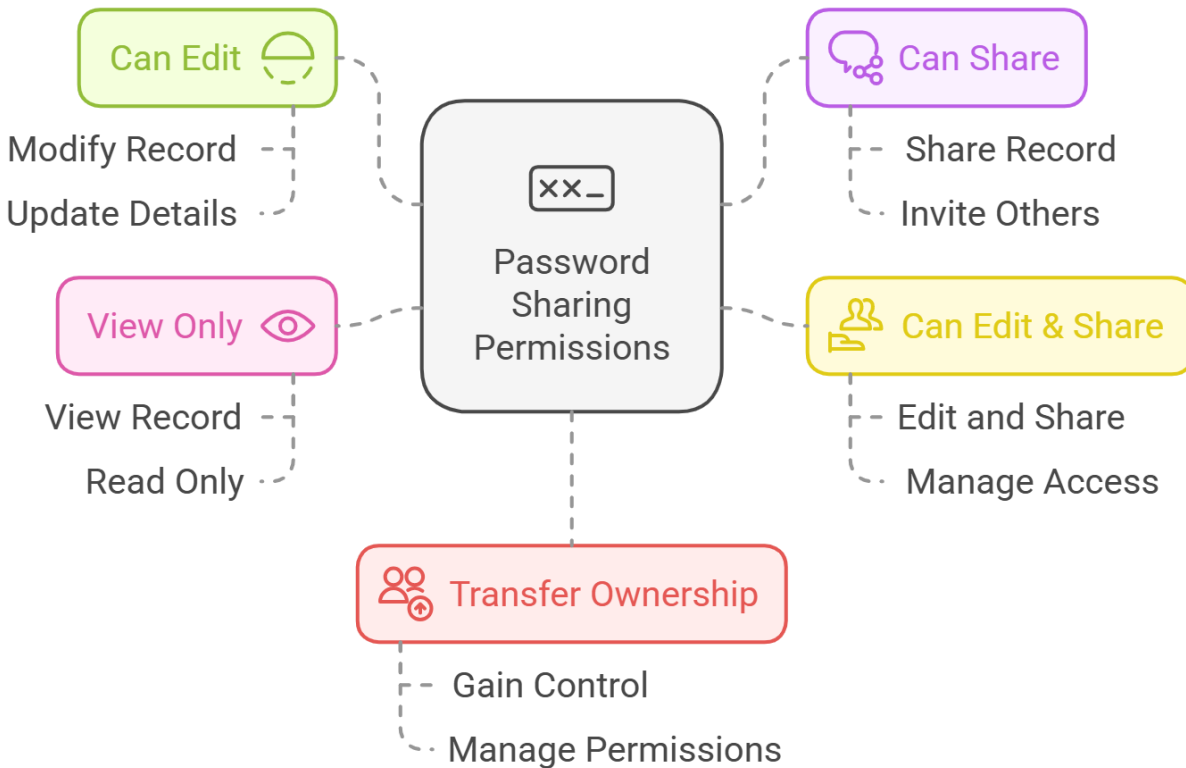
1. Share a Single Record

- While viewing a record, click **Share**.



- Enter the email(s) of the user(s) you would like to share the record with, then select their **permission type** from the dropdown menu (if they are not already a Keeper user, they will be invited to create an account via email).

Permission Name and Levels:



Using Keeper's Security Audit

The Security Audit screen gives the passwords stored in your vault an overall security score based on password strength. You can clearly view information about each record's password strength and reuse from this [screen](#).



1. Access the Security Audit Tool:

- From your vault dashboard, click on “**Security Audit**” (found on the leftside menu).

2. Review Your Audit Results:

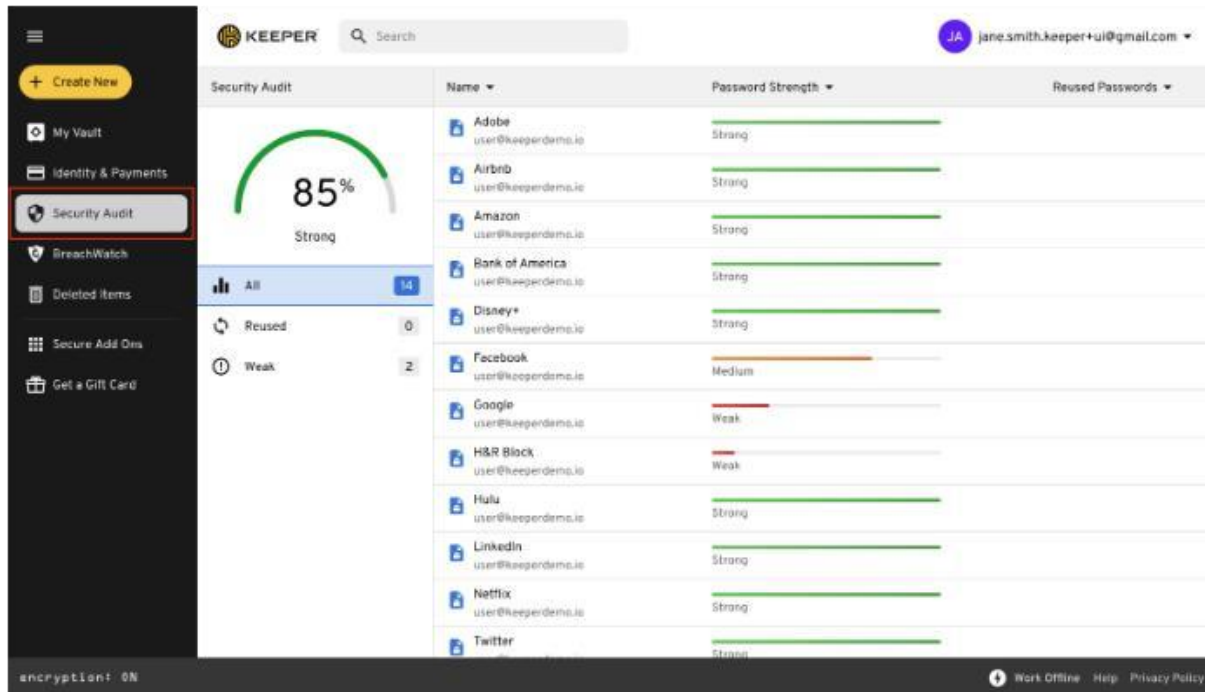
- The tool will display a summary of any passwords that need attention, such as weak passwords or passwords that have been used across multiple accounts.

3. Fix the Issues:

- Follow the recommendations provided by the audit, which may include updating weak passwords, enabling two-factor authentication, or changing compromised passwords.
- Keeper also offers a built-in password generator to help you create strong, unique passwords for each of your accounts.

Calculation of Security

The calculation of password strength and reuse is performed continuously from your vault across all platforms including Keeper Desktop, Web Vault, iOS and Android devices.



Keeper's password "strength" is a calculated score based on the complexity of the password, with a score rating between 0 and 100 according to the metrics below:

Very Weak: < 20 Weak: 20-40 Good: 40-60 Strong: 60-80 Very Strong: 80+

For more information on how Security Scores are calculated, visit the following [page](#).

You can easily view a record that contains a high-risk password by clicking on it from the provided list. To resolve the risk, you will be directed to change the password at the record's website and then update the corresponding record in your vault.

Final Notes and Reminders

- **Backup Your Vault:** It's recommended to backup your vault regularly and store backup copies securely.
- **Remember Your Master Password:** Keep your master password safe and consider using Keeper's biometric authentication for easier access on mobile devices.
- **Stay Secure:** Always enable two-factor authentication to add an extra layer of protection to your account.
- **Regularly Check the Security Audit:** Run the audit regularly to ensure your passwords remain strong and your accounts are protected.



Please note that if you forget your master password and lose your recovery phrase, you will not be able to login to your vault and Keeper Support will be unable to help you regain access.

By completing these steps, you're now fully set up with your Keeper Security password management account, with all your passwords securely stored and easy to access!

For other Keeper Security user guides, please visit this [link](#).

